

ATTACHMENT B

Items to be Seized

1. All evidence and records relating to violations of 18 U.S.C. § 875(c), those violations involving Google user vnice1937@gmail.com and Google user bennybrown6278@gmail.com, and occurring on about or after December 25, 2023, and continuing until on about or after February 20, 2024, including:
 - a. Records and information relating to the use of Google account vnice1937@gmail.com;
 - b. Records and information relating to the use of Google account bennybrown6278@gmail.com;
 - c. Records and information relating to explosives, including C-4, and records and information relating to the purchase or gathering of components for explosive devices;
 - d. Records and information relating to plans to purchase firearms, including any A-15 style firearms;
 - e. Records and information relating to plans to use firearms or explosives to kill or injure other individuals; and
 - f. Records and information relating to efforts to target illegal immigrants for acts of violence.
2. Computers or storage media used as a means to commit the violations described above;
3. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in

which is stored records or information that is otherwise called for by this warrant
(hereinafter, "COMPUTER"):

- a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;
- b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
- c. evidence of the lack of such malicious software;
- d. evidence indicating how and when the COMPUTER was accessed or used to determine the chronological context of COMPUTER access, use, and events relating to crime under investigation and to the COMPUTER user;
- e. evidence indicating the COMPUTER user's state of mind as it relates to the crime under investigation;
- f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;
- g. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;
- h. evidence of the times the COMPUTER was used;
- i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;
- j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;
- k. records of or information about Internet Protocol addresses used by the COMPUTER;
- l. records of or information about the COMPUTER's internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user

entered into any internet search engine, and records of user-typed web addresses; and

m. contextual information necessary to understand the evidence described in this attachment.

4. Routers, modems, and network equipment used to connect computers to the Internet.

5. Any and all firearms, including any AR-15 style firearms, and ammunition.

6. Explosive devices or other items that appear to be components for an explosive device, including C-4.

As used above, the terms “records” and “information” includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term “computer” includes all types of electronic, magnetic, optical, electrochemical, or other high-speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term “storage medium” includes any physical object upon which computer data can be recorded, including external and internal hard drives, flash drives, thumb drives, micro SD cards, macro SD cards, DVDs, gaming systems, SIM cards, cellular phones capable of storage, floppy disks, compact discs, magnetic tapes, memory cards, memory chips, and other magnetic or optical media.

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.